

**Notice of References Cited**

Application/Control No.

09/549,396

Applicant(s)/Patent Under  
Reexamination  
ROHATGI, PANKAI

Examiner

Taghi T. Arani

Art Unit

2131

Page 1 of 3

**U.S. PATENT DOCUMENTS**

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Name              | Classification |
|---|---|--|-----------------|-------------------|----------------|
|   | A | US-5,432,852                                     | 07-1995         | Leighton et al.   | 380/30         |
|   | B | US-5,646,997                                     | 07-0197         | Barton            | 380/23         |
|   | C | US-5,604,804                                     | 02-1997         | Micali            | 380/25         |
|   | D | US-5,608,801                                     | 03-1997         | Aiello et al.     | 380/46         |
|   | E | US-6,055,518                                     | 04-2000         | Franklin et al.   | 705/37         |
|   | F | US-6,226,743                                     | 05-2001         | Naor et al.       | 713/177        |
|   | G | US-6,311,271                                     | 10-2001         | Gennaro et al.    | 713/170        |
|   | H | US-5,754,659                                     | 05-1998         | Sprunk et al.     | 380/30         |
|   | I | US-5,625,693                                     | 04-1997         | Rohatgi et al.    | 380/23         |
|   | J | US-4,926,479                                     | 05-1990         | Goldwasser et al. | 380/23         |
|   | K | US-6,021,491                                     | 02-2000         | Renaud            | 713/179        |
|   | L | US-20003/0009666                                 | 01-2002         | Jakobsson         | 713/168        |
|   | M | US-6,532,540                                     | 03-2003         | Kocher            | 713/156        |

**FOREIGN PATENT DOCUMENTS**

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Country | Name | Classification |
|---|---|--|-----------------|---------|------|----------------|
|   | N |  |                 |         |      |                |
|   | O |  |                 |         |      |                |
|   | P |  |                 |         |      |                |
|   | Q |  |                 |         |      |                |
|   | R |  |                 |         |      |                |
|   | S |  |                 |         |      |                |
|   | T |  |                 |         |      |                |

**NON-PATENT DOCUMENTS**

| * |   | Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)   |
|---|---|---|
|   | U | Rohatgi Pankaj et al, How to Sign Digital Signature, I.B.M. T.J. Watson Reseach, Febuary 24, 1998   |
|   | V | Sivio Micali et al., On-Line/Off-Line Digital Signature, Proceedings of Crypto89.   |
|   | W | Digital Signature for Flows and Multicast, Chung Kei Wong et al., Department of Computer Sciences, The University of Texas a Austin, June 14, 1999. |
|   | X | Bruce, Schneier, Applied Cryptography, Second Edition, Pages 185-187, Published by John Wiley & Sons, INC, 1996.                                    |

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

**Notice of References Cited**

Application/Control No.

09/549,396

Applicant(s)/Patent Under  
Reexamination  
ROHATGI, PANKAI

Examiner

Taghi T. Arani

Art Unit

2131

Page 2 of 3

**U.S. PATENT DOCUMENTS**

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Name   | Classification |
|---|---|--|-----------------|--------|----------------|
|   | A | US-4,309,569                                     | 01-1982         | Merkle | 178/22.08      |
|   | B | US-  |                 |        |                |
|   | C | US-  |                 |        |                |
|   | D | US-  |                 |        |                |
|   | E | US-  |                 |        |                |
|   | F | US-  |                 |        |                |
|   | G | US-  |                 |        |                |
|   | H | US-  |                 |        |                |
|   | I | US-  |                 |        |                |
|   | J | US-  |                 |        |                |
|   | K | US-  |                 |        |                |
|   | L | US-  |                 |        |                |
|   | M | US-  |                 |        |                |

**FOREIGN PATENT DOCUMENTS**

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Country | Name | Classification |
|---|---|--|-----------------|---------|------|----------------|
|   | N |  |                 |         |      |                |
|   | O |  |                 |         |      |                |
|   | P |  |                 |         |      |                |
|   | Q |  |                 |         |      |                |
|   | R |  |                 |         |      |                |
|   | S |  |                 |         |      |                |
|   | T |  |                 |         |      |                |

**NON-PATENT DOCUMENTS**

| * |   | Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)   |
|---|---|---|
|   | U | Adrian Perrig, The BiBa One-Time Signature And Broadcast Authentication Protocol, University of California, Berkeley, Digital Fountain, ACM 1-58113-385-5/01/0011, 2001         |
|   | V | Josh Benaloh, One-Way Accumulators: A Decentralized Alternative to Digital Signatures, Advances in Cryptology Eurocrypt '93 LNCS, vol. 765, pp. 274-285, Springer-Verlag, 1994. |
|   | W | Marcel Waldvogel et al., The VersaKey Framework: Versatile Group Key Management, IEEE Journal on Selected Areas in Communications, vol. 17, No. 9, September 1999.              |
|   | X | J. BLACK et al., UMAC: Fast and Secure Message Authentication, Advances in Cryptology- CRYPTO '99 [7].  |

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.